Journal of Education Technology and Information System Vol (02) Ed (01) P.31-43 (2026)
Received June 2025 / Revised December 2025 / Accepted February 2025

Journal of Education Technology and Information System

https://journal.unesa.ac.id/index.php/jetis/

An Evaluation of ICP Blockchain System for Decentralized Certificate Verification: A Case Study at Maxy Academy

Febrian Daffa Eka Putra[1*], Dwi Fatrianto Suyatno[1]

[1] *Universitas Negeri Surabaya, Surabaya, Indonesia*
febrian.21032@mhs.unesa.ac.id , *dwifatrianto@unesa.ac.id*

Abstract. The falsification of digital competency certificates has become a growing concern in online education and training institutions, potentially undermining institutional credibility and employer trust. Maxy Academy, which provides digital skills training through online classes and bootcamps, currently lacks a dedicated mechanism for verifying certificate authenticity. This study focuses on the design and evaluation of a certificate authenticity verification system that utilizes the Internet Computer Protocol (ICP) Blockchain. The system was developed using the Rapid Application Development (RAD) approach and implements file hash-based verification to detect certificate authenticity, along with verification history logging and decentralized identity authentication through Internet Identity. Functional testing was conducted using Black-Box Testing, while system performance in distinguishing authentic from counterfeit certificates was evaluated using a Confusion Matrix based on a controlled test dataset comprising genuine and altered certificates. The evaluation results indicate that the system successfully distinguished authentic certificates from counterfeit ones under controlled testing conditions. These findings suggest that blockchain-based verification mechanisms have the potential to help institutions improve the reliability of digital certificate validation processes. This study contributes a practical case study of ICP Blockchain adoption for certificate verification in an educational training context.

Keywords: Blockchain-based Verification, Digital Certificates, Certificate Integrity Verification, Decentralized Systems, Educational Technology, Internet Computer Protocol.

1. Introduction

Competency certificates serve as formal evidence of learning achievement, completion of educational processes, professional expertise, and participation in training programs or organizations (Widjaja, 2022). In the digital era, however, the rapid development of information technology has been accompanied by an increasing number of counterfeit competency certificates. These fraudulent practices enable individuals to obtain certificates without undergoing proper learning or assessment processes and, in some cases, through illegal buying and selling transactions (Jaafar et al., 2024). This issue is not merely theoretical; in June 2020, law enforcement authorities uncovered a large-scale forgery syndicate that produced 5,041 fake seafarer skill certificates. The perpetrators illegally inserted certificate identification numbers into the Ministry of Transportation's centralized database, causing the forged certificates to appear legitimate within the official system (Infopublik, 2022).

The proliferation of counterfeit certificates has serious implications for organizations and employers, particularly during recruitment processes. When job applicants present fraudulent competency certificates, companies may recruit individuals whose actual skills do not match their documented qualifications, thereby decreasing workforce quality and increasing organizational risk (Lutfiani et al., 2022). Despite these challenges, certificate authenticity verification is still commonly performed using traditional, institution-centered methods, where documents must be manually

submitted and validated by issuing organizations. This process has been shown to be inefficient, time-consuming, and difficult to scale, especially when handling large volumes of certificates (Lutfiani et al., 2022). Although several institutions have attempted to improve verification mechanisms, many existing solutions remain highly dependent on human involvement, resulting in slow verification cycles and potential human error (Muhammad et al., 2022).

In Indonesia, technological efforts to address certificate fraud have been implemented, such as the Electronic Certificate Verification System (SIVIL) developed by the Directorate General of Higher Education, Research, and Technology (DITJEN DIKTIRISTEK). While SIVIL provides a digital verification mechanism for academic certificates, its centralized data storage architecture introduces vulnerabilities, including increased exposure to cyberattacks and risks associated with single points of failure (Azhar et al., 2024). These limitations highlight the need for alternative verification approaches that can improve data integrity, transparency, and system resilience.

Blockchain technology has been widely proposed in prior studies as a potential approach to addressing some limitations of centralized certificate verification systems, particularly in terms of data integrity and transparency. Blockchain enables decentralized data storage, immutability, and transparent record-keeping, making unauthorized modification of certificate data significantly more difficult (Vaher et al., 2025). Previous studies have demonstrated that blockchain-based verification systems can reduce the risk of certificate forgery and improve verification efficiency (Hari Hara Kumar et al., 2024). Among emerging blockchain platforms, the Internet Computer Protocol (ICP) Blockchain represents a third-generation blockchain architecture that offers improved scalability and performance compared to earlier platforms such as Ethereum. ICP Blockchain enables decentralized applications to operate without reliance on traditional servers or centralized cloud infrastructure, while maintaining responsiveness comparable to conventional web applications (Li et al., 2023). However, despite the growing number of studies on blockchain-based certificate verification, most existing research primarily emphasizes system design or conceptual frameworks, with limited empirical evaluation conducted in real institutional settings. Furthermore, the practical adoption of newer blockchain platforms such as Internet Computer Protocol (ICP) in educational or professional training institutions remains underexplored, highlighting the need for applied case studies that evaluate both system functionality and verification performance in real-world contexts (Naseem et al., 2025).

Maxy Academy is an institution that develops competencies through online classes and bootcamp programs, collaborating with various partners to prepare skilled human resources for the digital technology sector. Over the past two years, Maxy Academy has conducted 15 bootcamp batches, each involving approximately 100 participants, resulting in a substantial number of digital competency certificates issued. However, the increasing prevalence of certificate forgery has raised concerns regarding the potential misuse of Maxy Academy's certificates. These concerns are exacerbated by the absence of a dedicated platform for verifying certificate authenticity, which creates opportunities for forgery and complicates validation processes for industry partners. If left unaddressed, this situation may negatively affect institutional credibility, partner trust, and prospective participant interest.

Given these challenges, this study aims to design and evaluate a certificate authenticity verification system based on the Internet Computer Protocol (ICP) Blockchain for use at Maxy Academy. The proposed system aims to support certificate verification via a decentralized mechanism that uses file hash comparisons. By evaluating the system's functionality and its ability to distinguish authentic certificates from counterfeit ones, this study seeks to provide empirical insights into the practical application of ICP Blockchain for digital certificate verification in educational training institutions. The findings are expected to contribute to the growing body of research on blockchain-based credential verification and offer practical implications for institutions facing similar challenges.

Accordingly, this study is guided by the following research questions: (RQ1) How can a blockchain-based certificate verification system utilizing the ICP Blockchain ensure integrity-based

authenticity verification under controlled experimental conditions? And (RQ2) How does the proposed system perform in distinguishing authentic and counterfeit digital certificates within a structured testing scenario?

Despite the advantages of blockchain technology in ensuring data immutability and transparency, several limitations have been identified in prior studies. Blockchain-based certificate verification systems generally rely on deterministic data representations, such as cryptographic hashes, which restrict their ability to evaluate the semantic validity or contextual authenticity of digital credentials. In addition, scalability constraints, transaction latency, and reliance on off-chain data integrity remain ongoing challenges, particularly when such systems are deployed beyond controlled experimental environments. These limitations indicate that blockchain-based approaches should be positioned as integrity verification mechanisms rather than comprehensive solutions for detecting all forms of credential fraud.

2. Methods

2.1 Research Design

This study adopts a design-and-evaluation research approach, focusing on the development and empirical evaluation of a blockchain-based certificate authenticity verification system. The Rapid Application Development (RAD) methodology was selected as the system development framework due to its emphasis on iterative design, rapid prototyping, and continuous user involvement (Riadi et al., 2024). In addition to system development, this study incorporates functional testing and performance evaluation to assess the system's ability to distinguish authentic certificates from counterfeit ones.

2.2 System Development Method

Rapid Application Development (RAD) is a software development methodology that emphasizes short development cycles, iterative prototyping, and active user involvement. RAD was selected in this study due to its suitability for developing systems that require rapid feedback and continuous refinement. The RAD process applied in this study consists of four main stages: Requirement Planning, User Design, Construction, and Cutover (Mulyati et al., 2024).

- Requirement Planning

In this stage, problem identification was conducted based on a literature review and semi-structured interviews with representatives from Maxy Academy. Based on the findings, functional and non-functional system requirements were defined. Functional requirements include authentication for administrators and partners, certificate upload functionality, certificate authenticity verification through file hash comparison, and access to verification history. Non-functional requirements include PDF-only file acceptance, a responsive user interface, ease of use for non-technical users, and integration with Internet Identity and the ICP Blockchain to ensure data integrity.

- User Design

At this stage, system design was developed with user involvement to ensure alignment with user needs. Unified Modeling Language (UML) diagrams were used to model system functionality and user interactions, while wireframes were designed to visualize interface layout and navigation.

- Construction

The construction stage involved implementing the designed system into a functional web-based application. The backend was developed in Motoko, and the frontend in React, with Visual Studio Code as the development environment. Certificate file hashes were generated and stored on the ICP Blockchain to ensure data integrity and immutability.

- Cutover

The cutover stage focused on system testing and deployment readiness. At this stage, functional and performance evaluations were conducted to ensure that the system operated as intended.

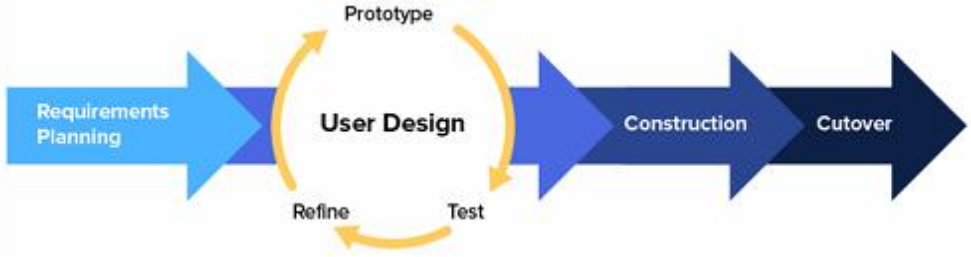

Figure 1. RAD Development Model

2.3 Data Collection and Testing Procedure

System testing was conducted during the cutover phase using two evaluation methods: Black Box Testing and Confusion Matrix–based performance evaluation. Black-Box Testing was employed to verify whether system functionality operated according to predefined requirements (Ramadan et al., 2025). Testing scenarios covered core features, including login, certificate upload, certificate verification, access to verification history, and certificate download. The testing process was performed by the researcher and three IT staff members from Maxy Academy to reduce individual tester bias.

For performance evaluation, a controlled dataset consisting of authentic and counterfeit certificates was used. A total of 30 certificates were prepared for each tester: 15 authentic certificates issued by Maxy Academy and 15 counterfeit certificates created by modifying the certificate content while preserving file format consistency. This balanced, synthetic dataset was intentionally used to ensure methodological clarity and controlled evaluation, rather than to represent real-world distributions of certificate submissions.

2.4 Data Analysis Technique

The system's ability to distinguish authentic certificates from counterfeit ones was evaluated using a Confusion Matrix, which classifies verification outcomes into True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN). Based on these values, evaluation metrics including accuracy, precision, recall, and F1-score were calculated (Park et al., 2025).

It is important to note that this evaluation focuses on functional correctness and verification capability within a controlled testing environment, rather than on large-scale deployment performance or real-world fraud prevalence. The results are interpreted as indicative of system effectiveness under defined experimental conditions.

3. Results and Discussion

3.1 System Functional Testing Results

Black-Box Testing was conducted to evaluate whether the developed system functions as intended in accordance with the predefined functional requirements. The testing covered core system features, including authentication via Internet Identity, certificate uploads by administrators, certificate authenticity verification via file hash comparison, verification history access, and certificate download functionality. The testing process was performed by the researcher and three IT staff members from Maxy Academy to reduce individual tester bias. The results indicate that all tested functionalities operated as intended, with no functional errors identified. These findings demonstrate that the system meets its functional specifications and is ready for operation under the defined testing conditions.

3.2 System Development Outcomes

3.2.1 Requirement Fulfillment Results

The development outcomes demonstrate that the system successfully fulfills the functional and non-functional requirements identified for Maxy Academy. All defined functional requirements were implemented and validated through system testing, including authentication for administrators and partners, multi-file certificate upload by administrators, certificate data management, access to verification history, and certificate authenticity verification using file hash comparison. The system accurately compared uploaded certificate hashes with stored records and displayed verification results as "Verified" or "Not Verified," as intended. Regarding non-functional requirements, the system meets the specified technical criteria. The application restricts uploads to PDFs, ensures a responsive user interface across mobile and desktop devices, and provides an intuitive interface suitable for non-technical users. Integration with Internet Identity enables secure authentication, while the use of Internet Computer Protocol (ICP) Blockchain ensures data integrity and authenticity. These results indicate that the system effectively satisfies the defined requirements and is suitable for its intended operational context.

3.2.2 Interface Implementation Results

The implemented user interface reflects the intended design outcomes derived from user-centered requirements. The interface realization is guided by Unified Modeling Language (UML) diagrams and wireframes, which serve as references for structuring user interactions and navigation flows. The resulting interface prioritizes clarity, accessibility, and ease of use for both administrators and partners.

The interface implementation ensures that users can intuitively access system features without extensive training. Clear navigation elements, consistent layouts, and responsive design principles contribute to a user-friendly experience. These characteristics are particularly important given the involvement of non-technical users in certificate verification and administrative processes.

3.2.2.1 Use Case Diagram

The Use Case Diagram illustrates the interactions between users and the system in executing specific system functions. It identifies the roles of administrators, partners, and public users, along with their respective access rights and permitted actions. Through this representation, the system boundaries and functional relationships are clearly defined, thereby supporting a structured, understandable system interaction model.

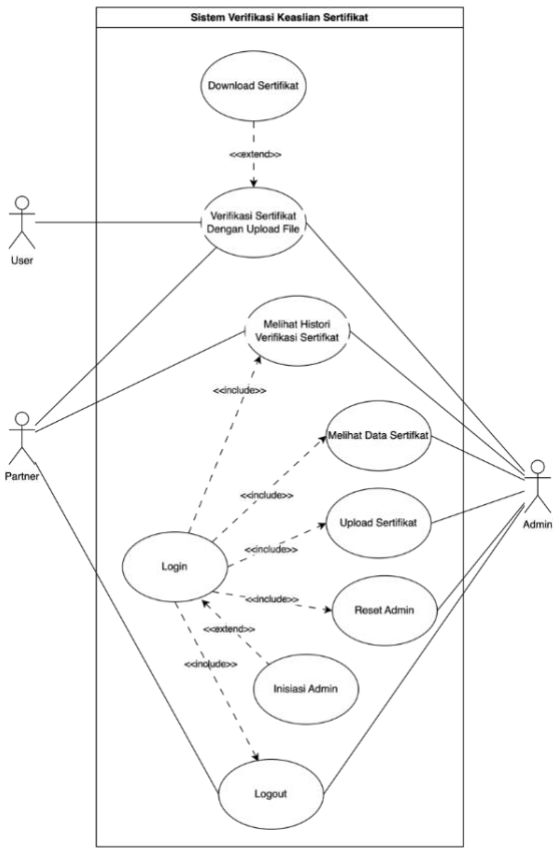

Figure 2. Use Case Diagram

3.2.2.2 Wireframe Design

Wireframes were used to represent the system's structural layout and navigation before full visual implementation. These wireframes focus on the placement of interface elements and functional components without incorporating detailed graphical design.

The wireframe design consists of three main pages accessible to general users and partners: the Certificate Authenticity Verification Page, which allows certificate verification without login; the Login Page, which enables administrators and partners to authenticate using Internet Identity; and the Partner Verification History Page, which allows partners to review certificate verification records.

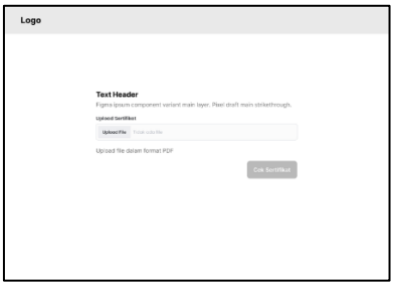

Figure 3. Certificate Verification Page

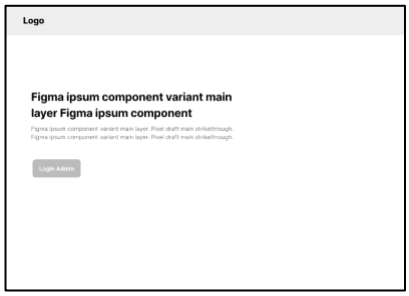

Figure 4. Login page

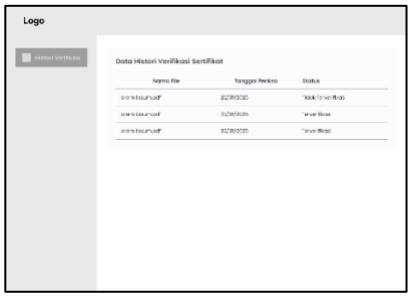

Figure 5. Partner Verification History Page

In addition, three pages are exclusively accessible to administrators: the Certificate Upload Page for uploading certificates along with course information, the Certificate Data Page for managing stored certificate records, and the Verification History Page for monitoring verification activities. These wireframes ensure functional completeness and logical navigation flow prior to deployment.

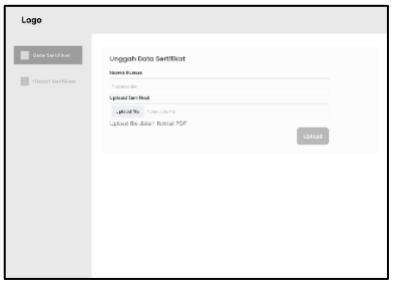

Figure 6. Upload Certificate Page

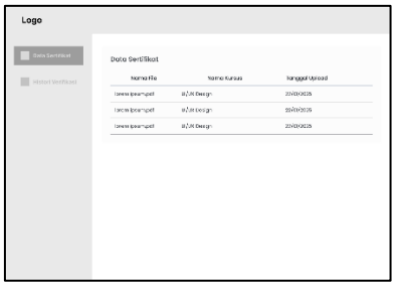

Figure 7. Certificate Data Page

Figure 8. Admin Verification History Page

3.2.3 Deployment Results

The deployment phase resulted in a fully functional web-based certificate authenticity verification system. All designed interfaces were successfully implemented and made accessible according to user roles and authorization levels. The deployed system demonstrates stable performance and consistent functionality across all pages.

3.2.3.1 Certificate Authenticity Verification Page

Figure 9. Certificate Authenticity Verification Page

The Certificate Authenticity Verification Page serves as the main entry point for users accessing the system. It allows users to verify certificate authenticity either individually or in bulk without requiring authentication. The responsive design enables certificate verification on mobile devices, allowing users to complete verification tasks anytime, anywhere.

3.2.3.2 Login Page

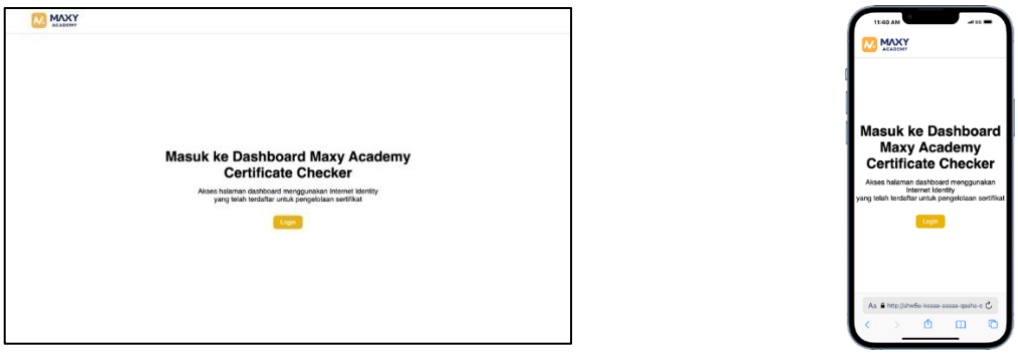

Figure 10. Login Page

The Login Page enables administrators and partners to access the system using Internet Identity authentication. This approach eliminates the need for traditional usernames and passwords,

enhancing security and simplifying the login process. The responsive design ensures accessibility across different devices.

3.2.3.3 Admin Initiation Page

Figure 11. Admin Initiation Page

The Admin Initiation Page is displayed when a logged-in Internet Identity account has not yet been registered as an administrator on the blockchain. Through this page, users can initiate administrator status by submitting their identity to the blockchain. This mechanism ensures controlled administrative access and secure role assignment.

3.2.3.4 Login Admin Page

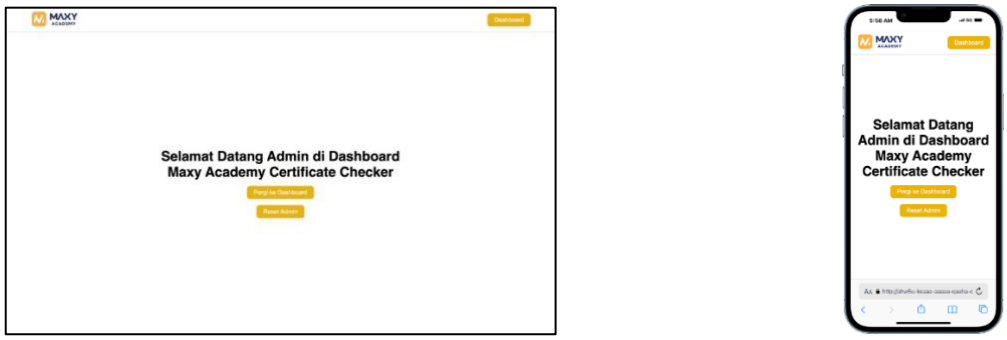

Figure 12. Login Admin Page

The Login Admin Page appears when the authenticated Internet Identity is recognized as an administrator. This page provides access to certificate data management features and administrative controls, including system reset functionality. The interface supports efficient administrative operations through a responsive layout.

3.2.3.5 Login Partner Page

Figure 13. Login Partner Page

The Login Partner Page is displayed when the authenticated Internet Identity is registered as a partner. From this page, partners can access the certificate verification history. The responsive design ensures partners can review verification records conveniently across devices.

3.2.3.6 Admin Certificate Data Page

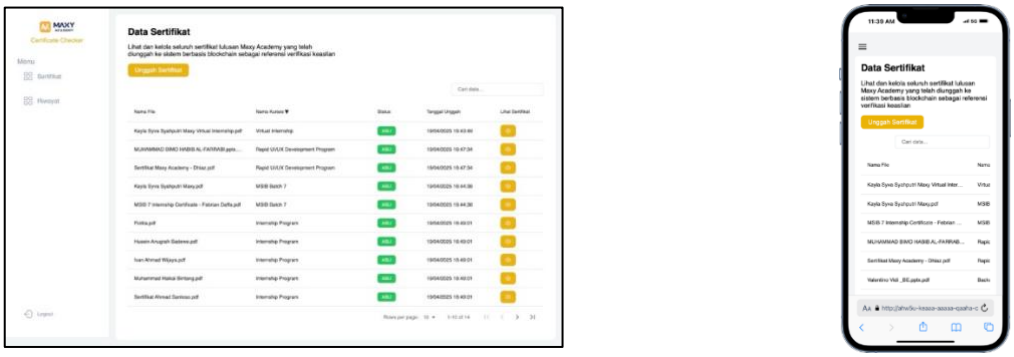

Figure 14. Admin Certificate Data Page

The Admin Certificate Data Page displays all certificate records stored on the blockchain. Administrators can view certificate details, including file name, course name, certificate status, and upload date. Additional features include detailed certificate viewing, data sorting, and keyword-based searching, supporting efficient data management and monitoring.

3.2.3.7 Upload Certificate Admin Page

Figure 15. Upload Certificate Admin Page

The Upload Certificate Admin Page enables administrators to upload certificate files in PDF format along with course information. The system supports batch uploads, allowing multiple certificates to be uploaded simultaneously. This functionality improves operational efficiency during certificate issuance.

3.2.3.8 Admin Verification History Page

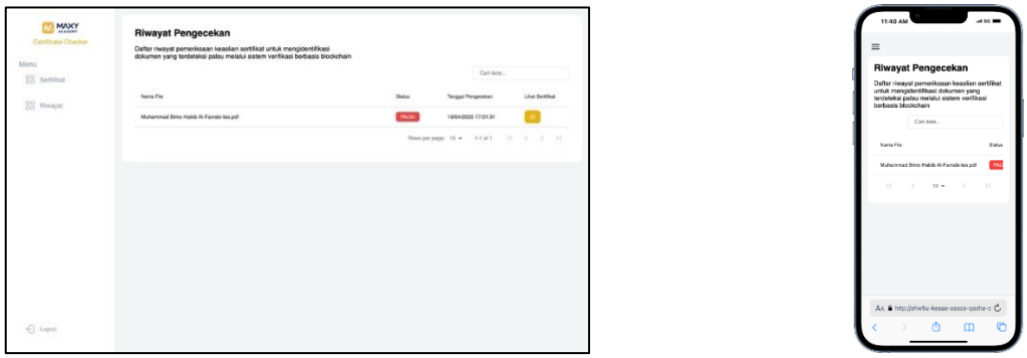

Figure 16. Admin Verification History Page

The Admin Verification History Page displays records of certificate authenticity verification activities. Administrators can review verification outcomes, access certificate details, and utilize sorting and search features to monitor verification trends and detect potential misuse.

3.2.3.9 Partner Verification History Page

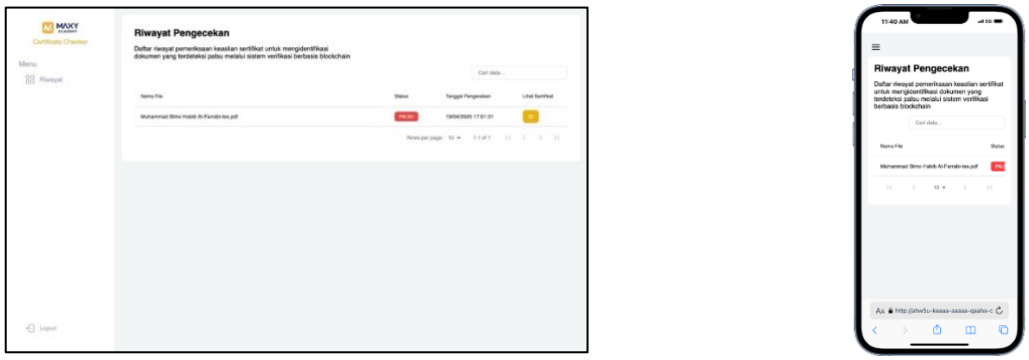

Figure 17. Partner Verification History Page

The Partner Verification History Page provides partners with access to verification records relevant to their activities. Users can view certificate status, verification dates, and detailed certificate content. This page supports transparency and accountability in certificate verification processes.

3.2.4 Cutover

During the cutover phase, the deployed system was tested using Black-Box Testing to ensure all functionalities operated as defined in predefined scenarios. The testing confirmed that all system features functioned as intended. Tested features included authentication, administrator reset, certificate upload, certificate data management, verification history access for administrators and partners, certificate authenticity verification, and certificate download. The results demonstrate that the system successfully transitioned from development to operational readiness, meeting all specified requirements and exhibiting stable functionality in a real-use environment.

3.3 Certificate Verification Performance Results

The system's accuracy in distinguishing between authentic and counterfeit certificates was evaluated using the Confusion Matrix method. Testing was conducted by the researcher and three IT staff from Maxy Academy, each testing 30 certificates (15 authentic and 15 counterfeit), for a total of 120 tests. The Confusion Matrix consists of four classification outcomes: True Positive (TP), where an authentic certificate is correctly identified as authentic; True Negative (TN), where a counterfeit certificate is correctly identified as counterfeit; False Positive (FP), where a counterfeit certificate is incorrectly identified as authentic; and False Negative (FN), where an authentic certificate is incorrectly identified as counterfeit. The results are summarized in the table below:

Table 1. Confusion Matrix Results

	Predicted: Authentic	Predicted: Counterfeit
Actual: Authentic	TP = 60	FN = 0
Actual: Counterfeit	FP = 0	TN = 60

Based on the confusion matrix values, the following evaluation metrics were calculated:

1. Accuracy

$$= \frac{TP + TN}{TP + TN + FP + FN}$$
$$= \frac{60 + 60}{60 + 60 + 0 + 0}$$
$$= 1$$
$$= 1 \times 100\%$$
$$= 100\%$$

2. Precision

$$= \frac{TP}{TP + FP}$$
$$= \frac{60}{60 + 0}$$
$$= 1$$
$$= 1 \times 100\%$$
$$= 100\%$$

3. Recall

$$= \frac{TP}{TP + FN}$$
$$= \frac{60}{60 + 0}$$
$$= 1$$
$$= 1 \times 100\%$$
$$= 100\%$$

4. F1-Score

$$= \frac{(2 \times Recall \times Precision)}{Recal + Precision}$$
$$= \frac{(2 \times 1 \times 1)}{1 + 1}$$
$$= 1$$
$$= 1 \times 100\%$$
$$= 100\%$$

These results indicate that the developed certificate authenticity verification system demonstrated correct classification behavior for all test cases within the defined controlled testing scenario, with no false positives or false negatives observed. This outcome reflects the deterministic nature of file hash–based verification, in which any modification to the certificate content results in a different hash value. However, these results represent system performance under controlled experimental conditions and are intended to demonstrate functional correctness rather than generalized real-world fraud detection performance.

3.4 Interpretation of Results

The results indicate that the proposed system achieved 100% accuracy, precision, recall, and F1-score in distinguishing authentic certificates from counterfeit ones within the controlled testing environment. This outcome can be attributed to the deterministic nature of file hash comparisons, in

which even minor modifications to certificate content result in different hash values. Consequently, the system consistently detected counterfeit certificates created through content alteration.

However, these results should be interpreted cautiously. The evaluation was conducted using a limited, controlled dataset, in which counterfeit certificates were generated by modifying authentic certificate files while preserving file format consistency. Therefore, the reported performance reflects system correctness under predefined experimental conditions rather than the real-world diversity of certificate forgery.

Furthermore, the system does not assess semantic validity or contextual correctness of certificate content, but focuses solely on file integrity verification through hash matching. As a result, the system is effective in detecting unauthorized modifications to issued certificates, but does not claim to address all possible fraud scenarios. Despite these limitations, the results demonstrate the functional correctness of the proposed system for integrity-based certificate verification within institutional certificate issuance contexts.

4. Conclusions

This study successfully designed and implemented a certificate authenticity verification system for Maxy Academy based on Internet Computer Protocol (ICP) Blockchain using the Rapid Application Development (RAD) approach. The developed system supports uploading certificates, authenticity verification via file hash comparison, tracking verification history, and secure authentication via Internet Identity. By leveraging ICP Blockchain, the system ensures data integrity, authenticity, and immutability within a decentralized environment.

System evaluation was conducted under controlled testing conditions using a dataset consisting of authentic and modified (counterfeit) certificates. The performance assessment using the Confusion Matrix showed that the system correctly distinguished authentic certificates from counterfeit ones within the defined testing scenario. This result reflects the correctness and reliability of integrity-based verification through deterministic file hash comparison.

It is important to note that the evaluation focused on functional correctness and integrity verification rather than comprehensive real-world fraud detection. Consequently, the reported results should be interpreted within the scope of the experimental setup. Despite these limitations, the proposed system demonstrates practical applicability for institutional certificate issuance and verification processes. The system has the potential to support Maxy Academy in strengthening certificate validation mechanisms, improving transparency, and reducing the risk of certificate misuse in educational and professional training contexts.

Acknowledgments

The author would like to express sincere gratitude to Maxy Academy for the support, collaboration, and facilities provided throughout the research process. Special thanks are extended to the academic advisor for their valuable guidance, feedback, and encouragement during the study. Appreciation is also given to friends who contributed directly or indirectly to the completion of this research. Lastly, heartfelt thanks to the author's parents and family for their continuous prayers, support, and motivation, which have been the driving force in completing this work.

References

Azhar, N. N., & Dharsana, I. M. P. (2024). Efektivitas penggunaan sertipikat elektronik dalam mencegah pemalsuan dokumen tanah. Jurnal Ilmu Hukum Humaniora dan Hukum Pidana (JIHHP), 5(2), 1080–1087. https://doi.org/10.38035/jihhp.v5i2

Hari Hara Kumar, G., Swapna, J., Sirisha, M., Siva Gowthami, K., Srinivas Kumar, B., & Info, A. (2024). Detection of Fake Certificate using Blockchain Technology. *International Journal for Modern Trends in Science and Technology*, *10*(09), 137–144. https://doi.org/10.46501/IJMTST1009022

Infopublik. (2022). *Polisi Bongkar Sindikat Pemalsuan Sertifikat Keterampilan Pelaut*. Infopublik.Id.

Jaafar, R. A., Alsaad, S. N., & Al-Kabi, M. N. (2024). Educational Certificate Verification System: Enhancing Security and Authenticity using Ethereum Blockchain and IPFS. *Al-Mustansiriyah Journal of Science*, *35*(1), 78–87. https://doi.org/10.23851/mjs.v35i1.1461

Li, A., Zichichi, M., Tang, S.-K., & D'Angelo, G. (2023). Modelling of the Internet Computer Protocol Architecture: The Next Generation Blockchain. *Lecture Notes in Networks and Systems*, *595*, 3–12. https://doi.org/10.1007/978-3-031-21229-1_1.

Lutfiani, N., Apriani, D., Ayu Nabila, E., & Lutfilah Juniar, H. (2022). Blockchain Frontier Technology (B-Front) Academic Certificate Fraud Detection System Framework Using Blockchain Technology. *Blockchain Frontier Technology (B-Front)*, *1*(2), 55–64. https://journal.pandawan.id/b-front/article/view/37

Muhammad, U. A., Aimufua, G. I. O., Abdullahi, M. U., & Muhammad, A. A. (2022). Certificate Generation and Verification System Using Blockchain Technology and Quick Response Code. *IOSR Journal of Computer Engineering*, *24*(1), 37–47. https://doi.org/10.9790/0661-2401023747.

Mulyati, S., Herdiansah, A., Taufiq, R., Prianggodo, D. Y., & Bukhori, S. (2024). Implementasi rapid application development (RAD): Studi kasus pengembangan sistem informasi sekolah Yayasan Al Abaniyah. JIKA (Jurnal Informatika), 8(2), 156–162.

Naseem, S., & Yong, T. (2025). Blockchain-based risk management in cross-border data supply chains: A comparative analysis of Alibaba and Infosys. Sustainability, 17(17), 7704. https://doi.org/10.3390/su17177704.

Park, S. J., Lee, H., Jeon, Y.-J., Woo, D. H., Kim, H.-Y., Kim, J.-O., & Jung, D.-H. (2025). Development of an RGB-GE data generation and XAI-based on-site classification system for differentiating Zizyphus jujuba and Zizyphus mauritiana in herbal medicine applications. Agriculture, 15(10), 1022. https://doi.org/10.3390/agriculture15101022.

Ramadan, M. N., Ramadhani, M. A. R., Handayani, C. T., Sulistiyani, E., & Budiarti, R. P. N. (2025). Implementation of black box testing and system usability scale on the Nurul Huda financial recording information system. Applied Technology and Computing Science Journal, 7(2), 136–149. https://doi.org/10.33086/atcsj.v7i2.8365.

Riadi, I., Yudhana, A., & Elvina, A. (2024). Analysis Impact of Rapid Application Development Method on Development Cycle and User Satisfaction: A Case Study on Web-Based Registration Service. *Scientific Journal of Informatics*, *11*(1), 81–94. https://doi.org/10.15294/sji.v11i1.49590.

Vaher, K., Simanjuntak, A., & Sugiharto, E. (2025). Securing academic records with blockchain technology: A data-driven approach for university management. Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi, 4(1), 52–62. https://doi.org/10.33050.

Widjaja, G. (2022). Memahami Makna Sertifikat Kompetensi Dan Sertifikat Profesi Menurut Peraturan Perundang-Undangan Yang Berlaku. *Cendikia : Media Jurnal Ilmiah Pendidikan*, *13*(2), 217–231.